UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA
Crim. No. 17-134 (WMW/DTS)

| | | |
|---|---|---|
| UNITED STATES OF AMERICA, | ) | |
| | ) | |
| Plaintiff, | ) | |
| | ) | |
| v. | ) | GOVERNMENT'S RESPONSE TO |
| | ) | DEFENDANT'S PRETRIAL MOTIONS |
| JOHN KELSEY GAMMELL, | ) | |
| | ) | |
| Defendant. | ) | |

The United States of America, by and through its attorneys, Gregory G. Brooker, Acting United States Attorney for the District of Minnesota, and Timothy C. Rank, Assistant United States Attorney, respectfully submits this omnibus response to defendant John Kelsey Gammell's pretrial motions [Docket Nos. 17-29].

## I. BACKGROUND

### A. Repeated DDoS Attacks Against Washburn Computer Group

Starting on July 30, 2015, the Washburn Computer Group (hereinafter "Washburn"), a computer company based in Monticello, Minnesota, began experiencing distributed denial of service ("DDoS") attacks targeting its website, www.washburngrp.com. (Criminal Complaint, Dkt. 1, at ¶7.) A DDoS attack is an attempt to make an internet-connected machine or network resource unavailable to its intended users, such as by temporarily or indefinitely interrupting or suspending services of a host connected to the internet, usually by shutting down a website or websites connected to the target of the DDoS attack. Washburn was subjected to periodic DDoS

attacks for more than a year, each time resulting in the temporary shut-down of its website. Washburn attempted to avoid the attacks by changing web hosting providers, purchasing mitigation services, and even changing the URL of its website (to www.washburnpos.com). The attacks continued through at least September 2016. *Id.*

Washburn's websites "wcgpdb.com" and "washburngrp.com" were knocked offline due to repeated DDoS attacks on the following dates:

- July 30, 2015;
- July 31, 2015;
- August 6, 2015;
- August 10, 2015;
- August 11, 2015; and
- August 12, 2015.

*Id.* ¶37.

On August 11, 2015, Washburn personnel received an email from l[redacted]_s[redacted]@yahoo.com[1] asking how everything was at Washburn:

[1] This Yahoo! email address is redacted in this filing because it contains the name of a former employee of Washburn whose identity Gammell used to falsely connect that employee with the DDoS attacks against Washburn and to conceal Gammell's involvement in those attacks.

**Hello from L[redacted]**

**From:** L[redacted] S[redacted] <l[redacted]_s[redacted]@yahoo.com>
**To:** [redacted]@washburngrp.com
**Date:** Tue, 11 Aug 2015 20:51:33 -0500
**Attachments:** MouseLaughing.gif (28.06 kB)

Hey [redacted],

How's everything at Washburn these days?

L[redacted]

*Id.* ¶15. The email contained an attached animation (.gif) from the cartoon "Tom and Jerry" of "Jerry" the mouse laughing:

FBI agents later learned from information provided by Yahoo! pursuant to a grand jury subpoena that the email account l[redacted]_s[redacted]@yahoo.com was created on August 11, 2015, with Gammell's cell phone number, 612-[redacted]-8609 (verified to be Gammell's through grand jury subpoena), listed as an alternate form of contact. *Id.* ¶10. The l[redacted]_s[redacted]@yahoo.com account was created approximately seven minutes before the email was sent to Washburn. *Id.* ¶37.

In an effort to prevent the ongoing DDoS attacks, on August 12, 2015 Washburn changed the IP addresses associated with their websites. However, on August 13, 2015 the DDoS attacks resumed, again knocking Washburn's website, "washburngrp.com," offline. In addition, on August 12, 2016, DDoS attacks targeted another Washburn

website, "washburnpos.com." These attacks knocked washburnpos.com offline until at least August 15, 2016. *Id.*

On or about August 13, 2015, Washburn began subscriptions with two different DDoS mitigation service providers in an attempt to mitigate the attacks. DDoS mitigation services use software that attempts to identify "normal" traffic to a website and block malicious traffic, such as traffic used to conduct a DDoS attack. The services utilized by Washburn were successful in blocking the attacks and the attacks subsided. *Id.* ¶38.

On October 6, 2015, heavy DDoS attacks resumed, again knocking the Washburn website offline. *Id.* ¶39. Also on October 6, 2015, Washburn personnel received an email from l[redacted]s[redacted]15@gmail.com,[2] asking again how everything was at Washburn and if any IT support was needed:

**From:** L[redacted] S[redacted] <l[redacted]15@gmail.com>
**To:** [redacted]@washburngrp.com
**Date:** Tue, 06 Oct 2015 14:12:50 -0500

[redacted]

You old Rascal. Hows everything going at Washburn? Need any IT support?

[2] This gmail email address is redacted in this filing because it contains the name of the same former employee of Washburn who Gammell had used in the Yahoo! email address referenced above, whose identity Gammell used to falsely connect that employee with the DDoS attacks against Washburn and to conceal Gammell's involvement in those attacks.

FBI agents later learned from information provided by Google pursuant to a grand jury subpoena that l[redacted]s[redacted]15@gmail.com was created on October 6, 2015, from IP address 75.161.68.161. Grand jury subpoena results showed that on October 6, 2015, IP address 75.161.68.161 was assigned to a Century Link internet account at Gammell's parent's home address, where Gammell was living at the time. Gammell's known cell phone number, 612-205-8609 (verified through grand jury subpoena), was also listed as the contact number on the account. The account was created approximately five minutes before the message was sent to Washburn personnel. *Id.*

On December 17, 2015, Washburn's website washburngrp.com was again hit with a DDoS attack. Logs provided by Washburn showed that IP address 64.145.94.119 was involved in the attack. IP address 64.145.94.119 is assigned to a company called IP Vanish, which is a US-based Virtual Private Network (VPN) subscription service that is used to anonymize the true source of incoming internet traffic. FBI agents later learned from information provided by Google pursuant to a grand jury subpoena related to Gammell's known email account, jkgammell@gmail.com, that on December 17, 2015, Gammell logged onto his gmail account from IP address 64.145.94.119. The same IP address, 64.145.94.119, was used in the DDoS activity targeting Washburn's website approximately seven minutes before logging into Gammell's email account, jkgammell@gmail.com. *Id.* ¶40.

**B. The Investigation**

In about mid-October 2015, FBI agents met with Washburn personnel after Washburn had reported to FBI that it was a victim of repeated DDoS attacks that had resulted in the takedown of Washburn's websites on multiple occasions. During that meeting, Washburn personnel informed the FBI agents about the details of the DDoS attacks, including the two emails received by Washburn which coincided with portions of the attacks and which purported to be from a former Washburn employee: the August 11, 2015 email from l[redacted]_s[redacted]@yahoo.com and the October 6, 2015 email from l[redacted]s[redacted]15@gmail.com. FBI Special Agent Brian Behm issued a number of grand jury subpoenas related to the two email accounts and eventually learned information that tracked the emails back to Gammell. Agent Behm thereafter contacted Washburn to determine whether they were familiar with Gammell. Agent Behm was informed that Gammell had previously been employed by Washburn as a soldering technician; that he had left to start his own soldering business; and that Washburn had talked to Gammell about contracting with Gammell to conduct soldering training of Washburn employees, but that there had been a dispute about what Washburn would pay for the training and so the training never took place. *Id.* ¶12.

Agent Behm conducted further investigation, eventually learning that Gammell had several social media accounts, including a Twitter account, @jkgammell. In October

2015, Gammell exchanged messages with two other Twitter users, during which Gammell demonstrated knowledge of DoS tools and solicited assistance in developing a DoS application. In one post, Gammell wrote to Twitter user @MaLrw3, "The LOIC is an entry level stresser and it gives up your IP unless you use a good VPN. Weak power." LOIC stands for "Low Orbit Ion Cannon," which is an open source application used to execute DoS attacks. Later, Gammell, using his Twitter account @jkgammell, wrote, "I need a pro who can code me a layer 7 stresser better than inboot, cstress, or vdos." Inboot, cstress, and vDOS are DDoS applications available for purchase on the internet. Agent Behm also learned that Gammell had attempted to obtain other DoS services using his email address jkgammell@gmail.com, in which he contacted an individual identified as CaillouBRAH, stating that he was looking for someone "to code me some stressers and booters code in Layer 4 and 7. I need something to at least hit the VIP packages of 50-80 Gbps of vDoS, Inboot, XYZ Booter, etc."

**1. jkgammell@gmail.com**

Thereafter, Agent Behm obtained a search warrant for jkgammell@gmail.com. Upon review of the records provided by Google, Agent Behm found numerous items indicating Gammell's involvement with DDoS activity. *Id.* ¶14.

From May 2015 to September 2016, Gammell expressed interest in, or made purchases from, the following seven websites offering DDoS-for-hire services:

"cstress.net," "inboot.me," "booter.xyz," "ipstresser.com," "exostress.in," "booterbox.com," and "vdos-s.com" (hereinafter "vDOS"). DDoS-for-hire websites offer users the ability to direct DDoS attacks at specified websites or IP addresses in exchange for a monthly subscription fee. The monthly subscription fee amount typically varies based on the duration and intensity of the attack. DDoS-for-hire websites are also often referred to as "booters" or "stressers." *Id.* ¶15.

In email communications with several people, Gammell identified cStress, vDOS, and booter.xyz as his favorite DDoS services to use. Gammell's relationship with vDOS will be detailed in the below section entitled "vDOS Records." The following are summaries of Gammell's relationship with the remaining six companies. *Id.* ¶16.

Gammell made multiple payments to the DDoS-for-hire service cstress.net via both PayPal and Skrill. Skrill is an online payment service based in the United Kingdom. In total, Gammell's payments to cstress.net totaled $234.93. In Gammell's jkgammell@gmail.com account, there were payment confirmations for the following payments to cstress.net, which include the date of payment, the amount paid, and the description of the monthly plan purchased:

a. August 3, 2015: $14.99 – "All Included;"

b. August 30, 2015: $29.99 – "Premium;"

c. October 2, 2015: $29.99 – "Premium;"

d. November 3, 2015: $39.99 – "Premium;"

e. December 8, 2015: $39.99 – "Premium;"

f. January 9, 2016: $39.99 – "Premium;"

g. June 5, 2016: $39.99 – "Premium."

*Id.* ¶17. The website cstress.net is not currently active, but it is available to review using archive.org. The main page of cstress.net as it appeared on March 21, 2016 contains a description of the "Premium" package, indicating that: (1) it can be used to "Stress Large Servers and Websites;" (2) it is capable of "Full Hour Stresses;" and (3) it provides "30Gbps of Dedicated bandwidth" and "Unlimited Boots." *Id.* ¶18.

On August 9, 2015, Gammell received an email from noreply@inboot.me providing a link to reset Gammell's inboot.me password. As noted above, inboot is a DDoS-for-hire service. On July 23, 2015, Gammell sent an email to DDoS-for-hire service booter.xyz via office@booter.xyz, stating he would like to order the monthly diamond membership. On December 13, 2015, Gammell sent another email to booter.xyz via office@booter.xyz, in which Gammell wrote that he is a current customer and wishes to upgrade, and he stated that booter.xyz has good service and he recommends them to others. *Id.* ¶19-20.

On May 22, 2015, Gammell received an email from DDOS-for-hire service ipstresser.com via email address no-reply@ipstresser.com requesting that he confirm his email address. *Id.* ¶21.

On May 27, 2016, Gammell received an email from noreply@exostress.in confirming the he had registered with DDoS-for-hire service exostress.in. *Id.* ¶22.

On July 2, 2016, Gammell received an email from noreply@booterbox.com providing a link to recover his account password. Gammell's username, which was embedded in the link, was indicated to be "Cunnilingus." As noted above, booterbox is a DDoS-for-hire service. *Id.* ¶23.

In addition to utilizing the DDoS-for-hire services as described above, Gammell also contacted several different individuals via email seeking assistance in starting his own DDoS-for-hire company. For example, on July 12, 2015, Gammell sent an email to an individual named Derek, who used the email address "thepicklator@aol.com." Gammell proposed a business partnership with Derek offering DDoS services, which would be advertised via Craigslist, Facebook, and Twitter. *Id.* ¶25. Gammell further proposed that DDoS attacks would be executed using monthly memberships maintained at cStress and vDOS. In the July 12, 2015 email to Derek, Gammell wrote:

> I would offer on Craigslist and Facebook services for doing DDoS. I will arrange an untraceable payment gateway and am also open to your suggestions. We would rent the following stresser/booter services on a monthly basis. These are the two most reliable and powerful "stresser"

> services. CStress has unlimited boots and VDoS limites [sic] to (40) per day at a length of 3600 seconds each (1 hour) using extremely powerful amplified DDoS. There services are completely untraceable so our IP's are totally protected. They uses dedicated services. http://cstress.net/index.php offers a $30./ month premium plan and https://vdos-s.com/ offers a 1 month Gold Plan for $50./ month. Combining these two concurrently on one website would be devastating, however, I am convinced that each one will do quite well on most sites that do not use DDoS mitigation. Between the software and DDoS services, are you interested? I cover all up front costs. All profits are split 50/50 on the net profit. Any minor up front costs or monthly membership costs for the DDoS memberships come off the top back to me from the gross profit. Everything up front and we create a financial management system in which we can both view at anytime via Dropbox or a secure cloud. Your anonymity is 100% guaranteed. Your name or involvement never leaves my mouth, guaranteed.

*Id.*

On July 23, 2015, Gammell sent an email to nofear.jonathan@hotmail.com after viewing a post by nofear.jonathan@hotmail.com on hackforums.net. Gammell asked if nofear.jonathan@hotmail.com could code a DDoS tool to target websites and servers. Gammell mentioned HOIC, which stands for "High Orbit Ion Cannon," an open source application used to execute denial of service attacks. Gammell wrote:

> I was checking out your post on hackforums. Tell me about DoSbox 4.5 Web Booter? Can you make me a viscous, stable booter that will drop websites and servers? Something far better than the HOIC that sucks up my system resources? I need a remarkable, stable, hard hitting beast. What do you have available for sale bro? Can you provide amlified [sic] NTS, DNS, SSDP, Layer 7, etc? I am a straight up business man. No bacon here. hit me up bro. My name is John.

*Id.* ¶26.

On January 18, 2016, Gammell sent an email to the.khaos.bringer@gmail.com, again looking for assistance in developing a DDoS tool. Gammell stated he would like the tool to work via an offshore internet service provider so it is not shut down if DDoS traffic is detected. Gammell noted in the email that he has memberships at vDOS, cStress, and booter.xyz. In the email to the.khaos.bringer@gmail.com, Gammell wrote:

> I am an Anon. I need the services of a qualified brother in the family. I need one or two very high end booter/stressers preferreably [sic] through an offshore ISP that will not trip if they suspect DDoS scripts. I prefer dedicated, multiple IP of course and here's the amusing part, I need it to hit with 200-300 Gbps with layer 4 and layer 7. I need to be able to drop Incapsula and that annoying Cloudflare who interfere with our digital world. I have a VIP membership to vDos at 50 Gbps, cStress at 30 Gbps and booter.xyz at 10 Gbps. I need more for my personal and want to look at the prospects of running a booter that exceeds the three previously mentioned. What would it cost me for an amazing booter and would you be interested in a business relationship where you get a percentage of each membership registraion [sic]?

*Id.* ¶27.

**2. vDOS Records**

As noted above, Gammell indicated in email communications that his preferred DDoS-for-hire services was vDOS. The vDOS website was shut down in 2016, and two Israeli men responsible for operating vDOS have been arrested and charged with computer crimes in Israel. *See* Brian Krebs, Israeli Online Attack Service 'vDOS' earned $600,000 in Two Years, Krebs on Security (September 8th, 2016, 12:04 pm), http://krebsonsecurity.com/ 2016/09/israeli-online-attack-service-vdos-earned-600000-in-

two-years; Brian Krebs, Alleged vDOS proprietors arrested in Israel, Krebs on Security (September 10th, 2016, 3:13 pm), http://krebsonsecurity.com/2016/09/alleged-vdos-proprietors-arrested-in-israel; Brian Krebs, Alleged vDOS Operators Arrested, Charged, Krebs on Security (August 9th, 2017, 11:43 am), https://krebsonsecurity.com/2017/08/alleged-vdos-operators-arrested-charged/.

In late July 2016, an internet security researcher provided the FBI with vDOS database records that the internet security researcher had obtained. The internet security researcher is well-known to the FBI agent to whom he provided the database, and FBI Special Agent Behm is also familiar with the internet security researcher's published work. *Id.* ¶28. The internet security researcher provided the vDOS database to FBI to assist in a criminal investigation into vDOS and its customers who used vDOS services to engage in DDoS attacks on victim websites, and the internet security researcher was neither directed to obtain the database nor compensated in any way for providing the database to law enforcement. *Id.* The database records provided information on the complete administration of vDOS, which includes user registrations, user logins, payment and subscription information, contact with users, and attacks conducted; the database records include information related to Gammell, who was a customer of vDOS. *Id.* The vDOS attack logs cover the time-period from approximately April 2016 to July 2016.

Agent Behm verified the authenticity of the vDOS database by comparing the information regarding Gammell in the database to information he obtained from accounts belonging to Gammell through grand jury subpoenas and search warrants. *Id.* ¶29. For example, the payment information for two of Gammell's subscription payments to vDOS contained in the vDOS database matches precisely with Gammell's PayPal records that Agent Behm obtained via grand jury subpoena, indicating that Gammell paid for the vDOS subscription using his PayPal account. *Id.* In addition, Agent Behm was able to match two of the monthly payments Gammell made for his vDOS subscription that were contained in the vDOS records with receipts for those payments that he located in Gammell's gmail account, jkgammell@gmail.com. *Id.*

Agent Behm searched the vDOS records for Gammell's known email addresses and usernames in an effort to identify vDOS accounts created and used by Gammell. His search yielded two accounts linked to Gammell's jkgammell@gmail.com email address. *Id.* ¶30.

Gammell's first vDOS account was created under the username "anonrooster," and the first observed activity under this username occurred on June 14, 2015. *Id.* ¶31. A payment of $39.99 was made on July 24, 2015 for the "1 Month Silver" plan. This payment was corroborated via a receipt from PayPal found in Gammell's jkgammell@gmail.com email account. There were no recorded DDoS attacks associated

with this account for the time period in the vDOS database, which, as noted above covered April 2016 to July 2016. *Id.*

Gammell's second vDOS account was created under the username "AnonCunnilingus," and the first observed activity under this username occurred on July 28, 2015. *Id.* ¶32. Gammell made multiple payments to vDOS via the "AnonCunnilingus" account, totaling $349.95. The transactions are listed as follows:

a. July 29, 2015 - $49.99, 1 Month Gold;

b. September 18, 2015 - $39.99, 1 Month Silver;

c. November 16, 2015 - $39.99, 1 Month Silver;

d. December 18, 2015 - $199.99, 1 Month VIP;

e. June 5, 2016 - $19.99, 1 Month Bronze.

*Id.* The payment for $199.99 on December 18, 2015 and $19.99 on June 5, 2016 were corroborated via Coinbase receipts located in Gammell's jkgammell@gmail.com email account. Coinbase is a BitCoin payment processing company. *Id.* ¶33.

A search of the vDOS database showed Gammell, using his "AnonCunnilingus" user account, logged into his vDOS account 33 times from IP address 75.161.68.161 over the time-period of October 2, 2015 to October 18, 2015. *Id.* ¶34. As noted above, grand jury subpoena results showed that in October of 2015, IP address 75.161.68.161 was assigned to a Century Link internet account at Gammell's parent's home address, where

Gammell was living at the time. IP address 75.161.68.161 was assigned to this account from August 28, 2015 to October 20, 2015. Gammell's vDOS activity overlaps with the email sent to Washburn on October 6, 2015 from l[redacted]s[redacted]15@gmail.com. As noted above, the email account l[redacted]s[redacted]15@gmail.com was created on October 6, 2015 using IP address 75.161.68.161. *Id.*

The vDOS database records show that Gammell used the "AnonCunnilingus" account to launch multiple DDoS attacks targeting approximately 20 IP addresses over the time-period of June 5, 2016 to July 5, 2016. *Id.* ¶35. Agent Behm was able to identify the entities to which those IP addresses were assigned, a sampling of which are set forth below. The analysis found that Gammell used the vDOS application to target a wide variety of websites, including those belonging to financial institutions (Wells Fargo Bank, JP Morgan Chase Bank, Hong Kong Exchanges and Clearing Limited); industrial and manufacturing companies (STI Electronics Inc., Kit Pack Co.); employment contracting companies (dmDickason); and government organizations (Dakota County Technical College (dctc.edu), Hennepin County (hennepin.us), Minnesota Judicial Branch (mncourts.gov)). *Id.*

Log files obtained from vDOS also contain communications between vDOS administrators and customers. On approximately August 2, 2015, Gammell, via his "AnonCunnilingus" account, provided feedback to vDOS on the success he had using their

service to knock targeted websites offline using a particular attack method, even websites supposedly protected with DDoS mitigation services. *Id.* ¶36. Gammell stated in this message that the target he was referencing did not have his permission to use the internet. The subject of his message was "Successfully dropped DDoS Mitigation." In the August 2, 2015 email, Gammell wrote the following:

> Dear Colleagues, This is Mr. Cunnilingus. You underestimate your capabilities. Contrary to your statement of "Notice! It apperas [sic] from our review that you are trying to stress test a DDoS protected host, vDos stresser is not capable of taking DDoS protected hosts down which means you will not be able to drop this host using vDos stresser(, Rackspace Hosting)." Port 53 utilizing UDP DNS amplification dropped the URL on the spot. Port 53 has unique exploitable vulnerabilities. As they do not have my consent to use my internet, after their site being down for two days, they changed their IP and used rackspace DDoS mitigation and must now be removed from cyberspace. Verified by downforeveryone. We will do much business. Thank you for your outstanding product :) We Are Anonymous USA.

*Id.*

**3. <u>Search Warrants in Colorado and New Mexico</u>**

During his investigation, Agent Behm learned that Gammell was living with his parents in Las Cruces, New Mexico, but that he was also working short-term jobs in locations outside of New Mexico. In May of 2017, Agent Behm learned that Gammell was working a short-term job in the Denver, Colorado area, and living at the Affordable Inns – Denver West, in Room 149. (Warrant for Search of Affordable Inns, Room 149, attached hereto as Exhibit A, Affidavit ¶42-43.) He also learned that Gammell was

driving a 2003 white Buick Century vehicle, with New Mexico license plates. *Id.* Accordingly, on May 26, 2017, Agent Behm sought a warrant authorizing the search of Room 149, as well as a warrant authorizing the search Gammell's vehicle, both of which were signed by the Honorable Kristen L. Mix of the United States District Court for the District of Colorado. *Id.* and Warrant for Search of 2003 Buick Century, attached hereto as Exhibit B.

**a. Affordable Inns - Wheat Ridge, Colorado**

On May 31, 2017, Agent Behm and other law enforcement executed the search warrant at the Affordable Inns – Denver West, Room 149, and arrested John Kelsey Gammell. Gammell was the sole occupant of the hotel room. During the search of the hotel room, FBI agents located several computers, smartphones, external hard-drives, and other electronic storage devices. In addition, FBI agents located parts for use in the building of AR-15 assault rifles, including an upper receiver, two lower receivers, a pistol grip, a trigger guard, and 15 high-capacity magazines. Gammell is prohibited from possessing firearms or ammunition based on his prior felony convictions, including his 1992 federal conviction for being a felon in possession of a firearm in violation of 18 U.S.C. §§ 922(g)(1) and 924(e)(1) (Crim. File No. 92-127 (HHM) (D. Minn.)). Gammell was released from prison on the felon in possession conviction in 2006, and he finished his period of supervision in 2010. Gammell is prohibited from possessing the AR-15

receivers because 18 U.S.C. § 921(a)(3) defines "firearm" to include "(A) any weapon . . . which will or is designed to or may readily be converted to expel a projectile by the action of an explosive" and "(B) the frame or receiver of any such weapon."

After his arrest, Gammell was interviewed by Agent Behm. Gammell claimed not to know what a distributed denial of service (DDoS) attack was, and denied any knowledge or involvement in executing DDoS attacks, including any attacks on Washburn. Gammell claimed that he was not aware of any online companies providing DDoS-for-hire services. Gammell stated that he did not recognize the names of the DDoS-for-hire services vDOS, cstress.net, or booter.xyz. Gammell also denied using his PayPal account to make purchases from DDoS-for-hire services. (May 31, 2017 Report of Interview of John Gammell, attached hereto as Exhibit C, at 1.)

**b. 2003 Buick Century**

Also on May 31, 2017, FBI agents in executed a search warrant on Gammell's 2003 white Buick Century, which was parked outside the Affordable Inns. The agents found a number of items, including a Garmin GPS device. FBI agents reviewed the GPS device for "Recent" locations, and learned, among other things, that the most recent address listed from New Mexico was for Discount Self Storage, a storage Facility in Las Cruces, New Mexico. (Warrant for Search of Discount Storage, attached hereto as Exhibit D, Affidavit ¶17.)

**c. Gammell's Parents' Residence - Las Cruces, New Mexico**

A search warrant was also executed on May 31, 2017 at the residence of Gammell's parents in Las Cruces, New Mexico, where Gammell had been living until traveling to Denver, Colorado for temporary employment. The warrant was signed on May 30, 2017 by the Honorable Gregory J. Fouratt of the United States District Court for the District of New Mexico. (Warrant for Search of Gammell's Parent's Residence, attached hereto as Exhibit E.) In the search, agents located a Dell desktop computer and a Verbatim 8 GB USB drive. In addition, agents located a gun case containing an owner's manual for a Heckler & Koch P2000 handgun. The serial number listed on the gun case was 116-039487. The gun was missing from the case. Gammell's father was interviewed by an FBI Agent and he stated that he had purchased the P2000 handgun for Gammell "before he left." (See Exhibit D, Affidavit ¶12.) As noted above, it is illegal for Gammell to possess any firearm.

**d. Westminster Arms - Arvada, Colorado**

On June 2, 2017, an FBI Agent interviewed an employee of Westminster Arms, a gun store in the Denver, Colorado area, concerning a receipt found during the search of Gammell's vehicle. The receipt listed two items, both described as "ACCESSORIES." One item was purchased for $99.99, and the second item was purchased for $114.99. The total amount of the transaction was $232.09. After reviewing the receipt, the employee

checked the area of the store where special ordered merchandise for customers was held. The employee matched the receipt found during the search to items special ordered and held for Gammell. The items were reviewed by the Agent and found to be two AR-15 accessories, a buttstock and a buffer tube. The items were paid in full by Gammell and were waiting for Gammell to pick them up. On June 26, 2017, a search warrant was issued by the Honorable Scott T. Varholak of the United States Court for the District of Colorado to seize the items purchased by Gammell from Westminster Arms. On June 28, 2017, FBI agents seized the items Gammell purchased from Westminster Arms, pursuant to the warrant.

**e. Tracer, Inc. - Golden, Colorado**

On June 2, 2017, an FBI agent spoke with the president of Tracer Inc., in Golden, Colorado, where Gammell had been working as a temporary contract employee. The FBI agent asked whether Gammell had a locker or other storage areas at Tracer Inc. and he was told that Gammell had a desk with drawers as well as a locker. The president of Tracer retrieved a box from one of the drawers. When he picked it up, he remarked, "Oh, I know what this is. It is ammunition." The box was a vacuum-sealed brown box with labeling "Nitro Express Shipping Super-Fast, Low Cost," and partial shipping label with address "Shipping Departm[portion torn off] (573) 445-6363, Midway USA, 5875 W. VAN HORN TAVERN RD" and the words "Cartridges Small Arms." On June 5, 2017, a search

warrant was issued to search and seize the box by the Honorable Craig B. Shaffer of the United States District Court for the District of Colorado. (Warrant for Search of Tracer, Inc., attached hereto as Exhibit F.) FBI agents found 420 rounds of 5.56 x 45mm full metal jacket rifle ammunition in the box. As noted above, it is illegal for Gammell to possess any ammunition.

**f. Discount Storage - Las Cruces, New Mexico**

On June 5, 2017, an FBI Special Agent Ryan Buckrop spoke with an employee of Discount Self Storage, located at 2499 El Camino Real, in Las Cruces, New Mexico, which was the most recent New Mexico address listed in Gammell's Garmin GPS unit. Exhibit D, Affidavit ¶17. The employee advised him that John Gammell rented a 5 ft. x 5 ft. storage unit at the facility, Unit Number 173. *Id.* As contact information for the rental, Gammell had provided an address of associated with his parent's residence; a phone number of 612-[redacted]-8609 (confirmed to be Gammell's cell phone number); and an email address of jkgammell@gmail.com. *Id.* When Gammell was arrested on May 31, 2017, he had several keys in his hotel room, including a key with the number 173 written on it in ink, which was the same number as the storage unit rented by Gammell. *Id.* On June 7, 2017, the Honorable Stephen M. Vidmar of the United States Court for the District of New Mexico issued a warrant for the search of Unit Number 173 at Discount Storage, and on June 9, 2017, FBI agents in New Mexico searched the unit pursuant to the warrant.

During the search, agents found USB thumb drives and other electronic storage media. Agents also located two handguns and hundreds of rounds of ammunition. One of the handguns was a Heckler & Koch P2000, serial number 116-039487 DE, matching the serial number on the gun case found at Gammell's parents' residence. The other handgun located was a Springfield Armory model 1911-A1, .45 caliber, serial number NM 435339.

4. **The Charges**

On June 5, 2017, Gammell was indicted in United States District Court for the District of Minnesota with one count of intentional damage to a protected computer, in violation of 18 U.S.C. §1030(a)(5)(A) and (c)(4)(B)(i). Gammell has also been notified that he will be charged in federal court in New Mexico and Colorado in connections with the firearms and ammunition he possessed in those states.

## II. THE DEFENDANT'S MOTIONS

The defendant has filed various boilerplate discovery motions (Docket Nos. 17-21). These motions appear to be precautionary measures meant to preserve potential arguments as opposed to raising any actual ongoing disputes regarding the government's discovery. In addition, the defendant has filed a motion for a bill of particulars, a motion for disclosure of informants, a motion to suppress evidence obtained by search warrant, and a motion to dismiss the indictment based on an allegedly unconstitutional statute (Docket Nos. 22, 24, 26, and 28.). The government will address the motions in the order they were filed.

## A. Defendant's Discovery Motions

### 1. Rule 16 Discovery [Docket No. 17]

The defendant moves the Court for an order for to disclose, produce, or permit inspection and copying of evidence and materials that fall within the scope of Rule 16 of the Federal Rules of Criminal Procedure. (Docket No. 17.) The government has made its Rule 16 disclosures by producing copies of various evidence and materials and making other materials available for inspection and copying. The government will continue to supplement its Rule 16 disclosures as additional materials come into its possession, as required by Rule 16(c).

The defendant's motion includes a request for an order of disclosure of expert witness information. The government is aware of its obligations under Rule 16(a)(1)(G) and intends to comply fully with the requirements of that rule. There is, however, no specific timing requirement included in Rule 16(a)(1)(G). Fed. R. Crim. P. 16 advisory committee's note, 1993 Amendments. The advisory committee's note provides that "although no specific timing requirements are included, it is expected that the parties will make their requests and disclosures in a timely fashion." *Id.* **The government respectfully requests that the Court order that expert disclosures for both parties, if any, be made 45 days before trial.** Such a timing requirement allows the parties sufficient notice of the expected testimony and time to prepare a focused cross-examination

of the expert. *See* Fed. R. Crim. P. 16 advisory committee's note, 1993 Amendments. Such an order would also provide the opposing party ample time to obtain a rebuttal expert and prepare a rebuttal report in advance of trial. **Accordingly, the government also requests that any rebuttal experts be noticed, and any rebuttal expert disclosures be produced to the opposing party, no later than 15 days before trial.**

**2. Disclosure of Evidence favorable to Defendant [Docket No. 18]**

The defendant moves the Court for disclosure of evidence favorable to the defendant. (Docket No. 18.) To the extent that defendant requests an order compelling the government to disclose any material in its possession that is favorable to him pursuant to *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), and their progeny, the motions are moot. The government has already complied, and will continue to comply, with *Brady*, *Giglio*, and related law. The government objects to the defendant's motion to the extent that it goes beyond the requirements of *Brady*, *Giglio*, and their implementing case law.

**3. Early Jencks Disclosure [Docket No. 19]**

The defendant moves the Court for early disclosure of Jencks Act materials. (Docket No. 19.) To the extent that defendant is requesting an order compelling the government to disclose any material in its possession that is favorable to them pursuant to *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), and

their progeny, the motions are moot. The government has already complied, and will continue to comply, with *Brady*, *Giglio*, and related law. The government objects to the defendants' motions to the extent that they go beyond the requirements of *Brady*, *Giglio*, and their implementing case law. It has been repeatedly and consistently held in this Circuit and District that the United States may not be required to make pretrial disclosure of Jencks material. *Finn v. United States*, 919 F. Supp. 1305, 1315 (D. Minn. 1995); *see also United States v. Ben M. Hogan Co.*, 769 F.2d 1293, 1300 (8th Cir. 1985); *United States v. White*, 750 F.2d 726 (8th Cir. 1984). "The Jencks Act requires that the prosecutor disclose any statement of a witness in the possession of the United States which relates to the subject testified to by the witness on direct examination." *United States v. Douglas*, 964 F.2d 738, 741 (8th Cir. 1992). "Although the United States need not produce Jencks statements prior to a witness' testimony on direct examination, the United States may agree to early discovery of Jencks material." *Douglas*, 964 F.2d at 741 n. 2. Accordingly, the United States objects to any court-ordered disclosure of such statements prior to the witnesses' testimony, but intends to provide all Jencks disclosures no later than 3 days before trial in this matter.

**4. Motion to Retain Rough Notes [Docket No. 20]**

The defendant moves the Court for an order requiring the law enforcement officials involved in the investigation of this case to retain and preserve their rough notes and

evidence gathered in the case. (Docket No. 20.) The government does not object to such an order. Notwithstanding the foregoing, the government does object to any request that agent rough notes be disclosed without further proceedings. Rough notes are generally not considered statements within the meaning of the Jencks Act. *United States v. Redding*, 16 F.3d 298, 301 (8th Cir. 1994) (concluding that rough notes are not a statement of witness as there was no evidence that the witness signed, adopted, or approved of agent's notes); *United States v. Shyres*, 898 F.2d 647, 657 (8th Cir. 1990) (defendant not entitled to discover Government agents' general notes from witness interviews). Nor are agent rough notes automatically discoverable as a "statement" of the agent. *See United States v. Simtob*, 901 F.2d 799, 808-09 (9th Cir. 1990) (defendant not entitled to discover testifying agent's destroyed rough notes of investigations as Jencks Act material when notes merely represented pieces of information put in writing to refresh memory); *United States v. Williams*, 875 F.2d 846, 853 (11th Cir. 1989) (defendant not entitled to discover agents' personal notes, contact sheets, witness lists, summaries of non-testifying witnesses' statements when bulk of material not relevant to subject matter of agents' testimony); *United States v. Bernard*, 623 F.2d 551, 558 (9th Cir. 1979) (Jencks Act not intended to cover rough surveillance notes).

**5. Disclosure of Rule 404(b) Evidence [Docket No. 21]**

The defendant has moved the Court for an order requiring the government to provide notice and make disclosure of any evidence it intends to offer under Federal Rule of Evidence 404(b). (Docket No. 21.) The government is fully aware of its notice and disclosure obligations under Rule 404 and intends on fully complying with that obligation. However, the government objects insofar as the defendants request immediate disclosure or disclosure 30 days or four weeks in advance of trial. *See* Fed. R. Evid. 404(b) advisory committee's notes, 1991 Amendments ("Other than requiring pretrial notice, no specific time limits are stated in recognition that what constitutes a reasonable request will depend largely on the circumstances on each case."). The government objects to the timing element of this request for the additional reason that it may lead to motions to suppress later-discovered Rule 404(b) evidence. The government proposes to notify the defense of Rule 404(b) evidence the government intends to use at trial no later than fourteen calendar days prior to trial, or upon learning of the existence of the evidence, whichever occurs later.

In addition, the government requests that any order be strictly drawn to require no more than what is encompassed by Rule 404(b). Specifically, Rule 404(b) does not encompass acts that are "intrinsic" to the charged offense. Fed. R. Evid. 404 advisory committee's notes, 1991 Amendments. If conduct of a defendant is an "intrinsic" part of any of the charged offense but could otherwise be considered a "bad act," then Rule 404(b)

does not contemplate that notice of such evidence be given. The distinction is an important one, as the defense may claim that the government must give notice of every "bad act" it intends to introduce, which is not so. *See United States v. Adediran*, 26 F.3d 61 (8th Cir. 1994) (standards applicable to evidence considered under Rule 404(b) do not apply to such "inextricably intertwined" evidence).

**B. Defendant's Other Motions**

**1. Bill of Particulars [Docket No. 22]**

The defendant has moved the Court for an order requiring the government to provide a bill of particulars. (Docket No. 22.) An indictment is "legally sufficient on its face if it contains all of the essential elements of the offense charged, fairly informs the defendant of the charges against which he must defend, and alleges sufficient information to allow a defendant to plead a conviction or acquittal as a bar to subsequent prosecution." *United States v. Wessels*, 12 F. 3d 746, 750 (8th Cir. 1993) (citing *United States v. Young*, 618 F.2d 1281, 1286 (8th Cir. 1980)). An indictment is sufficient "unless it is so defective that it cannot be said, by any reasonable construction, to charge the offense" for which the defendant has been indicted. *United States v. Hayes*, 574 F.3d 460, 472 (8th Cir. 2009). As a general matter, an indictment will be held sufficient if it tracks the language of the charging statute. *United States v. Sewell*, 513 F.3d 820, 821 (8th Cir. 2008). Conversely,

a bill of particulars is "not to be used to provide detailed disclosure of the government's evidence at trial." *Wessels*, 12 F.3d at 750.

The district court has broad discretion in deciding if a bill of particulars is needed. *United States v. Stephenson*, 924 F. 2d 753, 762 (8th Cir. 1991). A decision not to order the prosecution to file a bill of particulars will be reversed only if the defendant shows actual surprise at trial and concomitant prejudice from the trial court's denial of a bill of particulars. *United States v. Fleming*, 8 F.3d 1264, 1265 (8th Cir. 1993). *See also United States v. Sileven*, 985 F. 2d 962, 966 (8th Cir. 1993). Because of the emphasis on surprise to the defendant, a district court should consider, before ordering the prosecution to file a bill of particulars, whether the information the defendant seeks is available by another avenue, such as through discovery. *See generally United States v. Valentine*, 984 F. 2d 906, 908 (8th Cir. 1993) (motion for a bill of particulars denied as moot when the government indicated it had "opened its file" to the defendant). In this case, the government has opened its file to the defense, with the limited exception of some Jencks Act material and obviously non-discoverable material such as the prosecutor's work product. Moreover, the search warrant affidavits in this case provide a detailed roadmap of the government's case against the defendant. The indictment in this case is legally sufficient, and the defendant is safeguarded against surprise at trial by the voluminous discovery that the government has both sent to the defendant and made available for his

inspection. Accordingly, there is no need for a bill of particulars, and the motion seeking one should be denied.

**2. Disclosure of Informants and Witnesses [Docket No. 25]**

The defendant moves the court for an order requiring the government to disclose the identities of confidential informants and witnesses. (Docket No. 25.) Specifically, the defendant cites *Roviaro v. United States*, 353 U.S. 53, 61 (1957), *Brady*, and *Giglio* in support of the request for disclosure of the identity of the internet security researcher who provided the vDOS database to the FBI (*see* Section I.B.2, above).

The Supreme Court has recognized a government privilege to withhold the identity of confidential informants in certain situations. See *Roviaro*, 353 U.S. at 59. This privilege recognizes the obligation of citizens to report crimes, and "by preserving their anonymity, encourages them to perform that obligation." *Id.* The privilege gives way where the informant's identity is material to the defense. *Id.* at 60–61. The defendant bears the burden of showing that the informant's identity is material. *Carpenter v. Lock*, 257 F.3d 775, 779 (8th Cir. 2001). If the confidential informant is "an active participant or witness to the offense charged, disclosure will almost always be material to the accused's defense" and thus required. *Devose v. Norris*, 53 F.3d 201, 206 (8th Cir. 1995).

In this case, the internet security researcher was not an "active participant" in the crime charged in this case, or in any crime for that matter. Dkt. 1 ¶28. The internet

security researcher provided the vDOS database to FBI to assist in a criminal investigation into vDOS and its customers who used vDOS services to engage in DDoS attacks on victim websites, and the internet security researcher was neither directed to obtain the database nor compensated in any way for providing the database to law enforcement. *Id.*

The defendant argues that "the government should disclose the witness's criminal convictions; criminal acts for which charges could be brought; plea agreements; and other benefits." Dkt. 25 at 3. The government is happy to comply with this request: the witness has no criminal convictions; there are no criminal acts for which charges could be brought against the witness; and there are no plea agreements or other benefits. The internet security researcher is not a criminal defendant who has provided information in exchange for leniency or some other benefit, and instead is a concerned citizen who provided the vDOS database solely to assist the FBI in its investigation of DDoS activities. As the Affidavit of Special Agent Behm made clear, "the internet security researcher was neither directed to obtain the database nor compensated in any way for providing the database to law enforcement." Dkt. 1 ¶28.

The defendant suggests, in the title of Section II of his motion, that the informant "hack[ed] into Mr. Gammell's computer." Dkt. 25 at 3; *see also* 4 (asking the Court to order the government to disclose the identity of the witness "who broke into Mr. Gammell's computer"). This assertion is simply wrong. The security researcher provided a

database from vDOS, a company providing illegal DDoS-for-hire services. The database did not come from Mr. Gammell's computer. Mr. Gammell bought a subscription to vDOS and used it to initiate DDoS attacks on various websites. The identity of the internet security researcher need not be disclosed at this time.

At this point, in light of all of the other evidence demonstrating the defendant's criminal conduct in this matter, the government does not believe that it will call the internet security researcher to testify at trial in this matter. However, should that change, the government understands that it will be required to disclose the witness's identity in advance of trial.

### 3. Motion to Suppress [Docket No. 27]

The defendant moves to suppress the searches of his hotel room in Colorado, his vehicle, and his parents' residence based on his contention that those searches were "fruit of the poisonous tree," because law enforcement obtained warrants for those searches based in part on the vDOS records, which defendant claims were "purloined." Docket No. 27 at 2. He also moves to suppress any search that was based on the information obtained from the GPS device seized from defendant's vehicle.

#### a. Motion to Suppress Search Based on VDoS Records

Absent a legitimate expectation of privacy in the area searched or the items seized, a defendant cannot successfully assert a Fourth Amendment violation as a basis to suppress

evidence obtained by the search or seizure. *United States v. Bach*, 310 F.3d 1063, 1066 (8th Cir. 2002). As described above, the vDOS records did not come from the defendant's computer, or from any location in which he had an expectation of privacy. An internet security researcher provided the database, which came from vDOS, a company providing illegal DDoS-for-hire services. Gammell bought a subscription to vDOS and used it to initiate DDoS attacks on various websites, but he has no expectation of privacy in the information in the vDOS records.

Under the third-party doctrine, an individual can claim "no legitimate expectation of privacy" in information that he has voluntarily turned over to a third party. *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979) (finding no right to privacy in dialed telephone numbers); *United States v. Miller*, 425 U.S. 435 (1976) (finding no right to privacy in bank records). The Supreme Court has reasoned that, by "revealing his affairs to another," an individual "takes the risk ... that the information will be conveyed by that person to the Government." *Miller*, 425 U.S. at 443. "'[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.'" *United States v. Wheelock*, 772 F.3d 825, 828 (8th Cir. 2014) (quoting *United States v. McIntyre*, 646 F.3d 1107, 1111 (8th Cir. 2011)).

The vDOS subscriber information in this case is the kind of third party information for which the Eighth Circuit has expressly concluded individuals have no expectation of

privacy. *Wheelock*, 772 F.3d at 828–29 (finding no expectation of privacy in Comcast subscriber information, and holding "With Comcast in possession of his subscriber data, Wheelock cannot claim a reasonable 'expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers.'") quoting *United States v. Suing*, 712 F.3d 1209, 1211–12 (8th Cir. 2013); *United States v. Perrine*, 518 F.3d 1196, 1204–05 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.") (cited with approval and quoted in *Wheelock*).

**b. Motion to Suppress Based on GPS Data**

The defendant also seeks to suppress any search resulting from the seizure of the GPS device from his vehicle. Gammell claims that "the warrant did not direct the agent, with required particularity, to seize the GPS, which was compartmentalized away from plain view." Dkt. 27 at 5. Gammell is simply wrong. The warrant for the defendant's vehicle permitted the search of the entire vehicle, and did not limit the search to that which was in plain view. Exhibit D, Attachment A. Moreover, the warrant permitted search and seizure of any "computer" or "storage medium" that could contain evidence of related to the subject offense. Exhibit B, Attachment B. The warrant did not need to identify the specific kind of device to be searched in advance, so long as the device fell within the

defined scope of the evidence to be searched. *See, e.g.*, *United States v. Horton*, 638 Fed. App'x 126, 128-29 (3d Cir. 2016) (affirming denial of motion to suppress cell phone evidence because cell phone fell within scope of "computer hardware, including, but not limited to, any equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical or similar computer impulses or data" authorized by warrant). As further defined in Attachment B to the warrant, the term computer "includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions . . . ." Exhibit B, Attachment B. To require any further specificity would place an undue burden of clairvoyance on law enforcement officers, who could not know in advance the storage and data processing devices their search would yield or where those devices would be located. Indeed, in several other searches in this case, FBI agents seized laptop computers, desktop computers, external drives, and other storage media – none of which were, or could have been, specifically anticipated.

The Garmin Nuvi 2869 GPS device was plainly within the scope of the warrant's terms because it is both a "computer" and a "storage medium." *See, e.g.*, https://buy.garmin.com/en-US/US/p/138361 (Garmin Nuvi 2869 overview) (last visited October 16, 2017). The device performs high-speed data processing for vehicle navigation using GPS signals and up-to-date street maps that are stored on the device's

memory. Users can enter in a desired address, which the device can look up in its memory and then determine the fastest route to the destination based on real-time road traffic analysis. It has a 6-inch touch-screen display, Bluetooth capabilities for calls, and voice-activated navigation. The device operates using proprietary Garmin software; contains internal memory and supports memory cards for additional data storage; logs travel history; and can transfer data to and from other computers. Indeed, the evidence objected to by the defendant in his motion – previous locations visited that were stored in the Garmin device's memory – demonstrates that it falls within the scope of the "storage device" provision of the warrant, which is defined as "any physical object upon which computer data can be recorded," including "hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media." Exhibit B, Attachment B at 3. Finally, the type of data located on the device was identified in the warrant, which explained "some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence." Exhibit B, Affidavit ¶48(b).

**4. Motions to Dismiss [Docket No. 29]**

The defendant moves to dismiss the indictment in this matter because, he claims, 18 U.S.C. § 1030 exceeds Congress's power to regulate interstate commerce and it is unconstitutionally vague.

As to defendant's contention that Section 1030 exceeds Congress's power to regulate interstate commerce, the defendant cites no on-point case in support of his argument, and, indeed, the main case he cites stands for precisely the opposite proposition. Although defendant cites *United States v. Trotter*, 478 F.3d 918 (8th Cir. 2007), which rejected a similar constitutional challenge to Section 1030, the defendant apparently misunderstands its holding. In *Trotter*, the defendant had been fired from his job at the Midland Division of the Salvation Army in St. Louis, Missouri, where he had worked as an information technology supervisor. After he left, Trotter used an internet account at his girlfriend's residence in St. Louis to gain access to the computer network of the Midland Division of the Salvation Army, which was also located in St. Louis. The sole issue on appeal in *Trotter* was whether the defendant's conduct, which was started on a computer in St. Louis and did damage to a computer also in St. Louis, implicated interstate or foreign commerce or communication. *Id.* at 920. Indeed, Trotter argued, as the defendant does here, that "because '[n]early all computers [these] days are used someway in interstate commerce through the [I]nternet or private networks,' the statute cannot possibly be so broad as to cover the computer network of a not-for-profit organization like the Salvation Army." The *Trotter* court soundly rejected this argument, concluding that "With a connection to the Internet, the Salvation Army's computers were part of 'a system that is inexorably intertwined with interstate commerce' and thus properly within the realm of

Congress's Commerce Clause power." *Id.* (quoting *United States v. MacEwan*, 445 F.3d 237, 245 (3rd Cir. 2006)). Courts in other circuits have reached similar conclusions. *MacEwan*, 445 F.3d at 245 (concluding that the "Internet is an instrumentality and channel of interstate commerce"); *United States v. Mitra*, 405 F.3d 492, 496 (7th Cir. 2005).

In this case, Washburn's website advertised its products and services *on the internet*. By definition, a website is on the *World Wide Web*. And, even in the small sampling of part of the website attached to the defendant's memorandum (Dkt. 29-3), it is clear that the website is there to facilitate commerce. The website states on the first screen "We Repair, Sell, Exchange and Buy" point of sale systems. It contains both an 800 number to contact Washburn, as well as a link to use the website to submit a request for a quote for Washburn's services. (Dkt. 29-3 at 2, 15 & 16.) In addition, the website lists dozens of products, from companies all over the world, which they service, repair, and sell. Finally, the DDoS activity in this case was initiated from a computer outside of Minnesota, utilizing both the defendant's own DDoS scripts from that computer as well as directing DDoS-for-hire services around the world to launch attacks, on websites hosted on servers outside the state of Minnesota, that were used by a Minnesota company. Under the holding of *Trotter*, the criminal conduct at issue in this case is well within Congress's power to criminalize. As the *Trotter* court held, "once the computer is used in interstate commerce, Congress has the power to protect it." *Trotter*, 478 F.3d at 922.

The defendant's vagueness challenge is also without merit, although the precise nature of his argument is itself so vague as to not be entirely clear to the government, and he cites no on-point cases in support of his contention. If defendant's claim is that he didn't know it would be illegal to engage in a multi-month campaign to disable several websites belonging to his former employer, that claim simply does not withstand analysis. Indeed, if he thought what he was doing was legal, why try to conceal it? Why create fake email accounts in the name of a different former employee? Why deny conducting the DDoS attacks against Washburn, or even knowing anything at all about DDoS attacks, when asked by Agent Behm? Why? Because the defendant knew very well that his conduct was illegal – as did Congress when it passed the law, see 139 Cong. Rec. S16421-03 (daily ed. Nov. 19, 1993) (Statement of Sen. Leahy) (expressing concern that "computer abusers ha[d] developed an arsenal of new techniques which result in the replication and transmission of destructive programs or codes that inflict damage upon remote computers to which the violator never gained 'access' in the commonly understood sense of that term"), and the courts in upholding it, *see Mitra*, 405 F.3d at 496 ("[The defendant's] problem is not that § 1030 has been turned in a direction that would have surprised reasonable people; it is that a broad statute has been applied exactly as written, while he wishes that it had not been. There is no constitutional obstacle to enforcing broad but clear statutes."); *cf. United States v. Cook*, 782 F.3d 983, 989 (8th Cir. 2015) ("When a person

does an act that he well knows to be a violation of some law, and when a statute is later interpreted to cover his conduct in a way that does not do violence to the ordinary understanding of the English language, the [Fifth] Amendment is not offended.").

The defendant also questions how some of the defined terms in the statute can be decided – asking "who decides what is a 'reasonable cost to any victim'?" and who decides if Gammell "knowingly" caused damage to Washburn? (Dkt. 29 at 9.) The answer is that a jury will decide those issues, after receiving appropriate instructions from the court, at the conclusion of any trial in this matter. Section 1030 is not unconstitutionally vague.

## CONCLUSION

For all of the reasons set forth above, the United States respectfully requests that the defendant's discovery motions be denied as moot and defendant's remaining motions be dismissed.

Dated: October 16, 2017

Respectfully Submitted,

GREGORY G. BROOKER
Acting United States Attorney

*s/ Timothy C. Rank*

BY: TIMOTHY C. RANK
Assistant U.S. Attorney

AARON R. COOPER
Trial Attorney, Criminal Division